JUMP by Uber

Marcel Porras
Chief Sustainability Officer
Los Angeles Department of Transportation
100 S. Main Street, Los Angeles, CA 90012

October 28, 2019

Dear Mr. Porras,

We received your October 25th letter, notifying us of alleged non-compliance with the Los Angeles Department of Transportation (LADOT) Dockless On-Demand Personal Mobility One-Year Permit Program, and that LADOT is mandating that we come into compliance on these outstanding matters or you will suspend our permit to operate in Los Angeles. We urge LADOT to continue to work towards, and not away from, solutions that both further next generation transportation solutions for the public and ground themselves firmly in privacy best practice. We believe that best in class data aggregation methods could deliver LADOT near-real time data - while protecting the identity of Los Angeles residents and our riders.

As the Dockless On-Demand Personal Mobility One-Year Permit Program has repeatedly been framed by LADOT as a pilot program, JUMP has consistently shared feedback with LADOT regarding how the program can better protect the data privacy and security of our riders, while supporting LADOT's desire to receive data to manage and enforce dockless mobility operators. For example:

1. **LADOT still asserts that geolocation trip data is not personally identifiable:** According to LADOT's current website, "MDS does not collect personally identifiable data."[1] This is directly counter to best practice. According to NACTO, "[E]nsuring that geospatial trip data is treated as personally identifiable information (PII) is an essential part of best practice data management."[2] This data is also defined as personally identifiable in California law in the California Consumer Privacy Act (CCPA). JUMP repeatedly met with LADOT to ask that you follow global best practice by identifying and handling this data as personal information. [exhibit A]
2. **LADOT did not initially have any rules limiting the sharing of this data:** When the pilot was launched, LADOT had not placed any limitations on sharing this data with other city agencies (including law enforcement), and had not considered how this data set could be accessed in full via public records requests, etc. After a series of exchanges with JUMP [exhibit A], and in response to growing concerns from leading privacy experts, LADOT adjusted its policy to place minimal limitations on how this data can be shared.
3. **LADOT did not have public privacy protocols in place before collecting sensitive trip data:** LADOT required the sharing of raw, real-time on-trip data *before* developing or publishing privacy principles about how this data would be used, shared, and stored. It was only after JUMP and privacy groups expressed concerns about this volume of data transfer in the absence of any oversight or accountability when LADOT chose to draft and publish public privacy principles.[3] And while we support LA's drafting and releasing these principles for public comment, they do little to

[1] Source: https://ladot.io/faq/ *"How is LADOT protecting citizen data and citizen privacy?"*
[2] Source: https://nacto.org/wp-content/uploads/2019/09/NACTO_Shared_Micromobility_Guidelines_Web.pdf
[3] Source: https://cdt.org/insight/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/

actually protect privacy or educate the public about what data LADOT is collecting and how it plans to secure the data from breach or misuse. [exhibit B + C] See pg. 3 for more detail below.

4. **LADOT did not take the necessary steps to put guardrails on how the city and its private-sector contractors use this data beyond policy justifications:** LADOT has repeatedly required all dockless mobility operators to provide access to this raw geolocation data to venture-backed companies that have expressed intent to monetize this data for additional commercial purposes. One example of this was LADOT's permit requirement that operators provide a token to Remix, despite the fact that Remix was not bound by a contract with LADOT that placed limitations on how they could use, copy, sell, or monetize personal location data either in or outside of their work for LADOT. Once JUMP and other operators protested, this requirement was removed from the permit requirements. [See exhibit D]

These are four examples of the ways we have directly engaged with LADOT to establish basic privacy and security protections for the responsible use and collection of this data. We are willing to continue working with LADOT to identify and develop solutions to enable responsible data sharing; as such, we want to take this moment to address the questions outlined in your Friday letter.

"In-Trip Telemetry"

On our October 23rd call, it was clear that LADOT and JUMP disagreed about the definition of telemetry data. In March 2019, LADOT and JUMP leadership agreed that "in-trip telemetry" data could be provided at 24-hr latency for the term of the permit. "In-trip telemetry" data was not defined by either JUMP or LADOT in this meeting. It is also not defined anywhere in the MDS specification or in the LADOT compliance guidelines.

For LADOT, "in-trip telemetry" is route data only, and does not include trip start or trip stop. As such, LADOT now says we are out of compliance because we are not providing the trip start and trip stop data in real-time. For JUMP, "in-trip telemetry" applies to all sensor data collected from a bike or scooter that is associated with a user's trip, including the precise geolocation data from the trip start, trip stop, and the entire route; as such we understood this could all could be provided with latency for the express purpose of protecting privacy. For LADOT to exclude the start and stop points corresponding to one's origin and destination—both of which can be easily reversed to reveal one's home or work address—not only conflicts with a standard definition of trip information, but also stands in stark opposition to their original promise to protect privacy with this revised requirement

On the call, we offered to engage privacy groups and industry experts to sit town with all of us to more clearly define in-trip telemetry, and provide a neutral ground to hopefully reach consensus, but LADOT was unwilling to do so. As you are aware, the MDS specification itself currently lacks a "data dictionary", which is leading to inconsistencies across cities, operators and aggregators, etc. JUMP has been working closely with the Society of Automotive Engineers (SAE), who is leading the development of performance metrics for micromobility, to bring increased definitional clarity to the industry.

LADOT's Privacy Principles

As noted briefly above, while we were pleased to see LADOT eventually take public and transparent steps to produce and release privacy principles, we do not see that LADOT *meaningfully* incorporated feedback from privacy experts on how to take these principles beyond aspirational statements.There remain a number of outstanding concerns, including:

- Only two changes were made to the Privacy Principles based on all public comments from industry *and* independent privacy experts. LADOT did not share who reviewed and decided which changes were incorporated and why.
- LADOT has yet to share a timeline for when these Privacy Principles will be fully implemented (published March 22, 2019). Right now they are a statement of intent, and have not been codified in any way. In the meantime, LADOT continues to collect this sensitive consumer location data.
- The privacy principles do not state that LADOT will not monetize this data. There is also nothing that prevents either LADOT or third parties from monetizing outputs of the raw data -- so even if direct access to the data is not granted, these principles do not prevent third parties from selling products produced from this data. This is not only inconsistent with the expectations of our customers, but it is also the kind of practice that the global community has shed light on as an invasion of consumer trust.
- LADOT did not make any changes to the MDS specification that accounted for or reflected the Data Protection Principles they published. For example: data minimization, retention, or aggregation processes or SLAs were not added to the Github.
- LADOT did not share their methodology for how these commitments would be carried out, and there are not clear enforcement mechanisms or repercussions for failing to do so in the current version of the Privacy Principles. For example, as it relates to data minimization:

  "Data minimization: LADOT will mandate data sets solely to meet the specific operational and safety needs of LADOT objectives in furtherance of its responsibilities and protection of the public right of way. a. Aggregation, obfuscation, de-identification, and destruction: Where possible, LADOT will aggregate, de-identify, obfuscate, or destroy raw data where we do not need single vehicle data or where we no longer need it for the management of the public right-of-way. b. Methodologies for aggregation, de-identification, and obfuscation of trip data will rely on industry best practices and will evolve over time as new methodologies emerge."

  This section does not clearly address:
  1. What LADOT's "specific operational and safety needs of LADOT objectives" are; it is impossible to evaluate if they are minimizing data without clear use cases;
  2. The use of "where possible" should be more clearly defined so that it is not utilized as a 'catch-all';
  3. Methodologies that will be used.

To our knowledge, LADOT has taken no actions to aggregate, destroy, or otherwise protect sensitive raw data as recommended in their Principles document.

- - -

JUMP is committed to providing transformative micromobility options to our customers and city partners. But doing so at the expense of consumer privacy should not be a pilot program permit demand. JUMP has shared robust and comprehensive data sets with LADOT as our regulator. We would continue to do so if this can be done in a way that ***also*** protects consumer privacy and data security. Our concerns were further validated by the California's Legislative Counsel Bureau's August 1st opinion that LADOT cannot require real-time location data as a condition of our permit and doing so violates California Electronic Communications Privacy Act (CalECPA).

JUMP by Uber

Given that we seem to have exhausted all other avenues to find a compromise solution, tomorrow we will file a lawsuit and seek a temporary restraining order in the Los Angeles Superior Court, so that a judge will hear these concerns and prevent the Los Angeles Department of Transportation from suspending our permit to operate.

We sincerely hope to arrive at a compromise solution that allows us to work constructively with the City of Los Angeles while protecting the data privacy and security of our riders.

Colin Tooze

CC:
Mayor Eric Garcetti
City Attorney Mike Feuer
Councilmember Gilberto Cedillo
Councilmember Paul Krekorian
Councilmember Bob Blumenfield
Councilmember David Ryu
Councilmember Paul Koretz
Councilmember Nury Martinez
Councilmember Monica Rodriguez
Councilmember Marqueece Harris- Dawson
Councilmember Curren Price
Councilmember Herb Wesson
Councilmember Mike Bonin
Councilmember John Lee
Councilmember Mitch O'Farrell
Councilmember Jose Huizar
Councilmember Joe Buscaino